Data Processing Agreement

Last updated: 8th August 2025

This Data Processing Agreement ("DPA") forms part of the Terms of Service or other written or electronic agreement (the “Main Agreement”) between:

GlueDog Limited, a company incorporated in England, with a registered office at Unit 3 & 5A, Lister Mill Business Park, Lister Close, Plymouth, PL7 4BA ("Processor", "we", "us", or "our") **and**

The Customer, as defined in the applicable service agreement ("Controller", "you", or "your")

(together, the “Parties”).

---

1. Definitions

Unless otherwise defined in this DPA, capitalized terms shall have the meaning given in the Main Agreement or under applicable Data Protection Laws.

- **“Data Protection Laws”**: All applicable laws relating to data protection, privacy, and the processing of personal data, including the UK General Data Protection Regulation (UK GDPR), EU General Data Protection Regulation (EU GDPR), and the Data Protection Act 2018.
- **“Personal Data”**: Any information relating to an identified or identifiable natural person.
- **“Processing”**, **“Data Subject”**, **“Data Controller”**, **“Data Processor”**, and **“Supervisory Authority”** shall have the meanings given in applicable Data Protection Laws.
- **“Master Agreement”:** The primary contract, terms of service, or written or electronic agreement between the Parties that governs the overall provision of services, under which this Data Processing Agreement is incorporated and forms part.

---

2. Scope and Purpose of Processing

2.1 The Processor provides API connectivity and integration services which involve processing of personal data on behalf of the Controller.

2.2 The Processor shall process personal data only on documented instructions from the Controller and only to the extent necessary to perform the Services defined in the Main Agreement.

2.3 The types of data processed may include:

- API data transmitted through our platform
- Logs of API requests (retained for up to 14 days)
- Staff names and email addresses
- Minimum necessary data required to support integrations

2.4 The categories of Data Subjects include:

- The Controller's staff or personnel
- End-users or customers whose data is passed through APIs

3. Provider Obligations

3.1 The Processor will only process Personal Data according to the Controller's documented instructions and will notify the Controller promptly if it believes any instruction violates Data Protection Laws.

3.2 The Processor will reasonably comply with written instructions from the Controller to amend, transfer, delete, or otherwise process Personal Data, or to stop or remedy any unauthorised processing.

3.3 The Processor will keep all Personal Data confidential and will not disclose it to third parties except as authorized by the Controller, required to perform the Services, or by law. If legally required to disclose, the Processor will notify the Controller beforehand unless prohibited.

3.4 The Processor will assist the Controller with Data Subject rights requests, data protection impact assessments, and consultations with authorities only to the extent reasonably necessary and within the scope of the Services, with additional support subject to separate agreement.

3.5 The Processor will inform the Controller of any significant changes to Data Protection Laws that may materially affect its ability to fulfill obligations under this Agreement.

4. Provider's Employees and Officers

4.1 The Processor shall ensure that all employees, officers, contractors, and agents who have access to Personal Data:

a) Are informed of the confidential nature of the Personal Data and are subject to written confidentiality agreements or obligations restricting their use and disclosure of the data;

b) Have received adequate training on Data Protection Laws and understand how these laws apply to their duties involving the handling of Personal Data;

c) Are aware of both the Processor's obligations under this Agreement and their own individual responsibilities under applicable Data Protection Laws.

5. Security

5.1 The Processor shall at all times implement appropriate technical and organisational measures to protect Personal Data against accidental, unauthorised, or unlawful processing, access, copying, modification, disclosure, loss, destruction, or damage.

5.2 These measures shall be appropriate to the risk involved and shall include, where applicable:

a) Pseudonymisation and encryption of Personal Data;

b) Ensuring ongoing confidentiality, integrity, availability, and resilience of processing systems and services;

c) The ability to restore availability and access to Personal Data promptly in the event of a physical or technical incident;

d) A process for regularly testing, assessing, and evaluating the effectiveness of these security measures.

6. Personal Data Breach

6.1 The Processor shall notify the Controller without undue delay and in any event within 72 hours of becoming aware of any of the following:

a) Loss, unintended destruction or damage, corruption, or unusability of part or all of the Personal Data. The Processor shall restore such Personal Data as soon as reasonably possible;

b) Any accidental, unauthorised, or unlawful processing of the Personal Data; or

c) Any Personal Data Breach.

6.2 Upon becoming aware of any such event, the Processor shall provide the Controller with the following information without undue delay:

a) A description of the nature of the event, including categories of Personal Data affected and approximate number of Data Subjects and records involved;

b) The likely consequences of the event; and

c) A description of measures taken or proposed to address the event, including steps to mitigate adverse effects.

6.3 Following any such event, the Controller shall lead the investigation, and both parties shall cooperate fully in the investigation process.

6.4 The Processor shall reasonably cooperate with the Controller at no additional cost, including by:

a) Assisting with any investigation;
b) Providing access to relevant facilities and operations;
c) Facilitating interviews with relevant personnel;
d) Providing all relevant records, logs, files, and reports; and
e) Taking reasonable and prompt steps to mitigate effects and minimise any damage resulting from the event.

6.5 The Processor shall not inform any third party of the event without the Controller's prior written consent, except where required by applicable law.

6.6 The Controller shall have sole discretion over whether to notify Data Subjects, regulators, law enforcement, or other parties, including decisions about the content, timing, and method of such notifications and whether to offer any remedies.

7. Cross-border Transfers of Personal Data

7.1 The Processor may transfer or otherwise process Personal Data outside the United Kingdom where necessary to provide the services under this Agreement.

7.2 The Processor shall comply with all applicable Data Protection Legislation in relation to any such transfer or processing of Personal Data outside the United Kingdom.

7.3 If the Processor is required by applicable law to transfer Personal Data outside the United Kingdom, it shall inform the Controller of such requirement before making the transfer, unless prohibited by law from doing so.

8. Subprocessors

8.1 The Provider may engage third parties ("subprocessors") to process Personal Data on its behalf under this Agreement, provided that:

a) The Provider enters into a written contract with each subprocessor containing terms substantially equivalent to those in this Agreement and compliant with applicable Data Protection Legislation, including appropriate technical and organisational security measures. Upon written request, the Provider will provide the Customer with relevant excerpts of such contracts;
b) The Provider maintains control and oversight of all Personal Data entrusted to subprocessors;
c) The contract with each subprocessor automatically terminates upon termination of this Agreement for any reason.

8.2 The Parties agree that the Provider shall be deemed to legally control any Personal Data practically controlled or possessed by its subprocessors.

8.3 As of the commencement of this Agreement, the Provider does not engage any subprocessors. The Provider may engage subprocessors in the future and will maintain an internal list of such subprocessors. The Provider will notify the Customer of any material changes in subprocessors upon request.

8.4 If a subprocessor fails to meet its contractual obligations under clause 8.1(a), the Provider remains fully liable to the Customer for the subprocessor's performance and compliance.

9. Complaints, Data Subject Requests and Third-Party Rights

9.1 The Provider will, at no additional cost to the Customer, use reasonable efforts to implement appropriate technical and organisational measures and provide such information as the Customer may reasonably request to assist the Customer in complying with:

a) Data Subjects' rights under applicable Data Protection Legislation, including but not limited to rights of access, rectification, erasure, objection, data portability, and restriction of processing; and
b) Any notices or assessments issued by the Information Commissioner or other relevant regulatory authorities.

9.2 The Provider shall notify the Customer promptly in writing upon becoming aware of any complaint, notice, or communication related directly or indirectly to the processing of Personal Data or either party's obligations under Data Protection Legislation.

9.3 The Provider will notify the Customer within five (5) business days if it receives a request from a Data Subject to access their Personal Data or exercise any other rights under applicable Data Protection Legislation.

9.4 The Provider agrees to cooperate with and provide reasonable assistance to the Customer, at no additional cost, in responding to any such complaints, notices, communications, or Data Subject requests.

9.5 The Provider will not disclose Personal Data to any Data Subject or third party except in accordance with the Customer's written instructions or as required by applicable law.

10. Term and Termination

10.1 This Agreement shall remain in full force and effect for as long as:

a) The Master Agreement remains in effect; or
b) The Provider retains any Personal Data related to the Master Agreement in its possession or control.

10.2 Any provision of this Agreement which by its nature is intended to survive termination or expiration of the Master Agreement, particularly those necessary to protect Personal Data, shall continue in full force and effect.

10.3 The Provider's failure to comply with the terms of this Agreement shall constitute a material and irremediable breach of the Master Agreement. In such case, the Customer may terminate the Master Agreement immediately by written notice to the Provider, without further liability or obligation.

10.4 If a change in applicable Data Protection Legislation renders either party unable to fulfill its obligations under the Master Agreement, the parties may agree to suspend Personal Data processing until compliance is restored. If the parties cannot achieve compliance within 30 days, either party may terminate the Master Agreement with at least 14 working days' written notice to the other party.

11. Data Return and Destruction

11.1 At the Customer's written request, the Provider shall provide the Customer, or a third party nominated in writing by the Customer, with a copy of or access to all or part of the Personal Data in the Provider's possession or control, in a format and on media reasonably specified by the Customer.

11.2 Upon termination or expiry of the Master Agreement, or earlier termination or cessation of the relevant service, the Provider shall, at the Customer's election, securely delete or return to the Customer all Personal Data processed under the Agreement and shall not retain any copies thereof, unless retention is required by applicable domestic law.

11.3 The Provider shall certify in writing to the Customer, within 30 days of completion, that it has securely deleted or destroyed the Personal Data in accordance with this clause

12. Records

12.1 The Provider shall maintain adequate written records of its processing activities involving the Personal Data, including details about access, control, and security measures applied, as well as the purposes of processing.

12.2 The Provider will use reasonable efforts to ensure these records demonstrate compliance with its obligations under this Agreement and applicable Data Protection Legislation.

12.3 The Provider shall cooperate with the Customer to the extent reasonably necessary to assist the Customer in meeting its record-keeping obligations under applicable Data Protection Legislation.

13. Notice

13.1 Any notice under this Agreement must be sent by email to the following contacts:

- To the Customer, at the email address registered to their account.
- For the Provider: Compliance Officer at data.protection@gluedog.ai

If either party changes their email address, they'll notify the other at least 7 days in advance. Emails sent without bounce-backs will be considered received the next business day at 9:00 am London time.

13.2 This doesn't apply to formal legal documents or dispute notices.

ANNEX I – Details of Processing

Nature and Purpose of Processing:

- Facilitation of API integrations between partner systems
- Logging and debugging of API calls
- Operational support and configuration of integration services

Types of Personal Data:

- Names and email addresses of staff
- Personal data transmitted via API integrations
- Technical log data

Categories of Data Subjects:

- Employees of the Controller
- End-users whose data is transferred via APIs

Duration of Processing:

- For the duration of the services provided under the Main Agreement and up to 14 days post-processing for logs

Sub-processors:

- A list of sub-processors is available upon request.